BUSINESS CONTINGENCY PLAN - Y2K

PAYROLL

PREPARED BY

LAUSD Information Technology Division

Table of Contents

POLICY AND STRATEGY

POLICY

The Y2K Business Contingency plan:

1. Ensure an organized and effective response in the event the Payroll System becomes inaccessible or inoperative due to Y2K.
2. Ensure continuity for the payroll system, until normal processing capability is restored.

STRATEGY

The strategy of the Payroll Y2K Contingency Plan is as follows:

1. Ensure that all relevant computer software and databases are duplicated and stored in a secure off-site location for use in recovery.
2. Provide alternate processing guidelines to support essential business functions and maintain cash flow during a computer disaster recovery period.
3. Publish an organized plan that can be used as a reference should disaster actually occur.
4. Identify responsibility to restore processing in the event of a loss.

EMERGENCY RESPONSE

Emergency Response identifies required tasks and responsibilities that: 1) must be addressed at the time a specific contingency occurs; or 2) are needed to establish temporary processing capabilities at another location. It contains actions assigned to specific individuals as well as Emergency Response Team that may perform individually or collectively during the Emergency Response Period, at the discretion of the Director, Information Technology Division.

RESPONSIBILITY	ACTION
1. Director, Information Technology Division	Determine if the Disaster Recovery and Business Continuity Plan will be activated.
2. Data Center Operations Manager	Initiate any reconstruction that might be required at a temporary data processing location.
3. Data Center Operations Manager	Document a chronological list of all key events surrounding the disaster emergency response actions and interim processing activities.

4.	Data Center Operations Manager	Expedite installation of new telephone/ communications systems as required.
5.	Deputy Director, ITD	Coordinate efforts between the computer and User communities until normal processing capability is restored.
6.	Deputy Director, ITD	Contact personnel on the Emergency Response Notification List (Appendix), as appropriate.
7.	Deputy Director, ITD	Refer to Minimum Office Requirements (Appendix) in the event it is necessary to set up temporary work locations.

SYSTEM PROFILE-PAYROLL

SYSTEM NAME: **PAYROLL SYSTEM**

SYSTEM DESCRIPTION: (KEY USER PROCESSES SUPPORTED BY APPLICATION)

The Payroll System is a software application that is used to process salary payments for all District Employees.

The Payroll Services Branch provides a variety of payroll services to the employees of the District.

The system provides processing of the following routines:

- Salary payments
- Cancellations
- Redraws
- Emergency payments
- Cash receipts

This contingency plan addresses the payroll application and other processes performed in the Payroll System. It is intended to cover problems arising from Y2K disruptions to automated systems and related equipment. It is not intended to address other contingencies such as those arising from earthquakes or other disasters. These are covered in our Disaster Recovery Plan.

KEY FILE UPDATES:

Job	Program	Description
A1107S01	A1107CXX	SORT ALL INPUT DATA FOR PROCESSING
A109MAJ1	A1109NXX	PROCESSES FUTURES: RELEASES OF HOLDS
A103MAJ1	A1103CXX	PROCESSES INPUT DATA UPDATES OR ACTIONS AND CHANGES
A1200S01	A1200CXX	UPDATES DEDUCTIONS AND MAJOR ASSIGNMENTS
A1ATES01	A1120CXX	UPDATES PAY RATES

KEY PAYROLL PROCESSES:

Program	Description
A0207V01	Create Control Ticket
A0202V99	Convert Payment Code
A0209V02	Sort all payroll input
A0209NV1	Name Check
A0211V38	Matrix and Validate Input
A0212V99	Create Input Listing by Div, Loc
A0215V24	Payroll Process
A0216V99	Create Payroll Exception
A03PCV04	Insert # Sign
A0224V43	Add Address to Payment File
A0226	Sort Payment File
A0217V36	Create Salary Warrant
A0218V17	Create APD Tapes
A0502V04	Salary Distribution
A0501V13	Salary Distribution
A0219V16	Detail Register
A0503V02	Salary Distribution
A0235V16	Warrant Register by Employee Number
A0234V16	Warrant Register by Location

KEY REPORTS:

Report Number	Description
RBT212R1	PAYROLL INPUT LISTING BY DIVISION
RBT216R01	PAYROLL RUN EXCEPTIONS BY DIVISION
RBT2116R1	PAYROLL EXCEPTIONS BY EMPLOYEE NUMBER
TS217WAR	WARRANTS
TS217SCS	SCOPE
A0217MAJ/SUP	GROSS PAY/WARRANTS > 10,000.00
A0218MAJ/SUP	ERROR/CANCELLATION APD REPORT
RBT219R1	WARRANT REGISTER BY EMPLOYEE DETAIL
RBT223R1	BANK RECONCILIATION LISTING
A02EZIMA/SA	NAME OR EMPLOYEE NUMBER ERROR

ONLINE INQUIRY CAPABILITY

There is no on-line access; everything is run by batch. The Payroll System relies on the Human Resources System (HRS) for employees personal and approved assignment data, the Payroll Time Reporting System (PTRS) for employees time reporting and on Data Entry to key other inputs (adjustments, deductions, tax information, etc) and documents manually written by Payroll.

APPLICATIONS DEPENDENT ON OUTPUT FROM THIS SYSTEM:

IFS
Job Cost Integrated Financial System

DATA SHEET

System Name: Payroll System

Computer:

Hardware: IBM 9121
Operating System: OS390: Version 2.5

Personnel:

Application Support:

- ***Deputy Director***

  Richard Overturf

- ***Senior Systems and Programming Analyst***

  Annie Lim,
  Bernie Meller

- ***Systems and Programming Analysts***

  Carl Branson
  Lawrence Clemons
  Steve Creswell
  Carol Garfield
  Dennis McDonie
  Cherrie Mitchell
  Odette Ricasa
  Glen Shono

- ***Assistant Systems and Programming Analyst***

  Patrick Bingham

Primary User: **Payroll Services Branch**

Normal Processing Frequency: Monthly

Special Forms: Pre-print warrants for Regular Payroll Issue
Pre-print warrants for Emergency Payroll Issue
Non pre-print warrants for Garnishment Issue
APD Stock for Issue of Automatic Pay Deposits

POTENTIAL IMPACT

Payroll System is down in January 2000

Impact on Students:

Because the system has no on-line functions and does not support students directly, there is no impact to the students.

Impact on Staff:

The impact to staff is the potential of not being paid or paid on time. The first payrolls of January, and there are three, will be addressed in the work-around plan of this contingency plan.

The next major impact in January is the 13th of January when payroll starts for the classified employees for a pay date of January 21, 2000.

Impact on Users and Technical Support:

The impact of the user (Payroll Services Branch) having to type up approximately 35,000 checks for the January 21, 2000 payday will be addressed as one option. The payroll system is impacted if the HRS, and PTRS systems are not available and if no data entry. HRS provides personal and assignment data for employees, PTRS provides time reporting data to pay the employees, and Data Entry provides the means that Payroll can make adjustments to employees.

> As of this date we have experienced one Y2K failure. The problem has been resolved. If any more problems should arise between now and cutover of the new year, they will be handled in the same timely manner by programming staff assigned.

Impact on Other Applications

Payroll would not be able to feed information to other Applications/hardware.

System Accessibility

The payroll system will be accessible as long as there are backup facilities available to programming staff.

INTERIM PROCESSING STRATEGY

Interim Processing Strategies summarize what will be done to ensure that vital business functions continue, in the event of a disruption in standard data processing capability.

Following is the Interim Processing Strategy applicable to this system:

Advance Payments (Accrual)

This interim processing strategy represents the advance planning necessary to insure the payment process for employees of the Los Angeles Unified School District.

Preparation:

- All locations that use PTRS for reporting time (including Job Cost) will be notified to print copies of their rosters and time report that were certified for the 0699 and 2400 pay periods.

- Instructions will be provided to locations regarding how to use the rosters and time reports should the system not be available for the classified payroll, scheduled to be paid January 21, 2000.

- ITD programming staff will produce a Warrant Register by location and will include an additional field for an EPA amount (95% of the next pay).

- ITD programming staff will add a new register to each of the payroll run streams for the 0699 pay period (pay date December 23, 1999); and for the 2400 pay period (pay date January 7, 2000) being run the last week of December except for the ESA payroll. These registers may be used later if the system is not available.

- ITD will backup the Payroll System before December 30, 1999.

- Payroll Branch will inquire of the availability of manual typewriters in the district schools or the availability of purchasing or leasing a large volume (approx. 75) in case there is no systems available to print checks. The Payroll Branch would type manual checks for the employees for the 0700 pay period pay date January 21, 2000 using the new warrant register by location with the EPA amount, that would be the amount of the warrants to be issued to employees.

- ITD to check on leasing generators or a mobile data center (Data Center on Wheels) before 30 September 1999.

- Request payroll to create warrants only for the first payroll of January. If there is no problem, the worst is that the employee on ADP would have to go to the bank. This affords us approximately a two weeks window to determine if there are any Y2K problems without affecting anyone.

INTERIM PROCESSING GUIDELINES

Interim Processing Guidelines highlight activities to be address in support of Interim Processing Strategies. Following are the Interim Processing Guidelines for this system in the event of a Y2k contingency.

A. Start Up

The following step should be taken in anticipation of implementing Interim Processing Guidelines.

- Assure backup of all key data files.
- Assure that a copy of the contingency plan is in the Data Center
- Have a list of all key personnel, including telephone number, page number and cellular phone number; include responsibilities.
- Assure that adequate supplies are available.

B. Interim Processing

The following activities need to be performed to assure payroll payments to LAUSD employees in the event of a disaster or interruption to normal business processing.

1. Run payroll processing the week of December 27th, creating both APD (automatic payroll deposit) and warrants.
2. Store the warrants (back room of Salary Delivery) until mailing on January 6th.
3. Test the wire transfer process on Monday, January 3, 2000; if wire transfers are not functioning, it must be corrected by Wednesday, January 5, 2000.
   - If the wire transfer process is not corrected by Wednesday, January 5, 2000, then a special Supplemental payroll would need to run Wednesday night, January 5, 2000, to cancel all APD payments from all three (3) payrolls and issue warrants for mailing, January 6, 2000. This is assuming that there are no pay process Y2K problems, and there is electricity.

- Depending upon the extent of the wire transfer problem and/or other Y2K problems, a tape may be FEDEX or hand delivered to the San Francisco Bank of America Branch.

- The System can be down eight days with minor impact. Payroll would have to generate emergency warrants manually. After eight days, there is a need to pay approximately 40,000 classified employees by January 21, 2000.

- If more Y2K problems arise due to repairs not being made, make necessary repairs in a timely manner, test and place into production.

- If there are any problems with the system, such as, Breaches of Security, System Performance Degradation, etc., operations will shut down system and notify system programmers to run diagnostic testing.

In addition to the above activities, the following activities will need to be performed if normal business activities are interrupted due to loss of electricity, environmental controls, breach of security, or communication.

1. Invoke the ITD Disaster Recovery Plan.

2. Move all payroll operations to the backup site. Or,

3. Contact the mobile data center (Data Center on Wheels) vendor (previously contracted with) to initiate delivery.

4. If the ITD Data Center, 450 N. Grand, is operational (generators in use), notify the time reporting locations that the training room on the second floor is available for entering labor time. Also, Personnel Offices would be notified that they could do their updates online. A schedule would be developed to accommodate the needs of the various offices/functions.

5. This scenario would eliminate the need for the Payroll Branch to manually create warrants.

CONTINGENCY PLANNING STEPS

The following charts, Contingency Plan Execution and Contingency Plan Coordination, shows the steps to be taken if the following Y2K events occur.

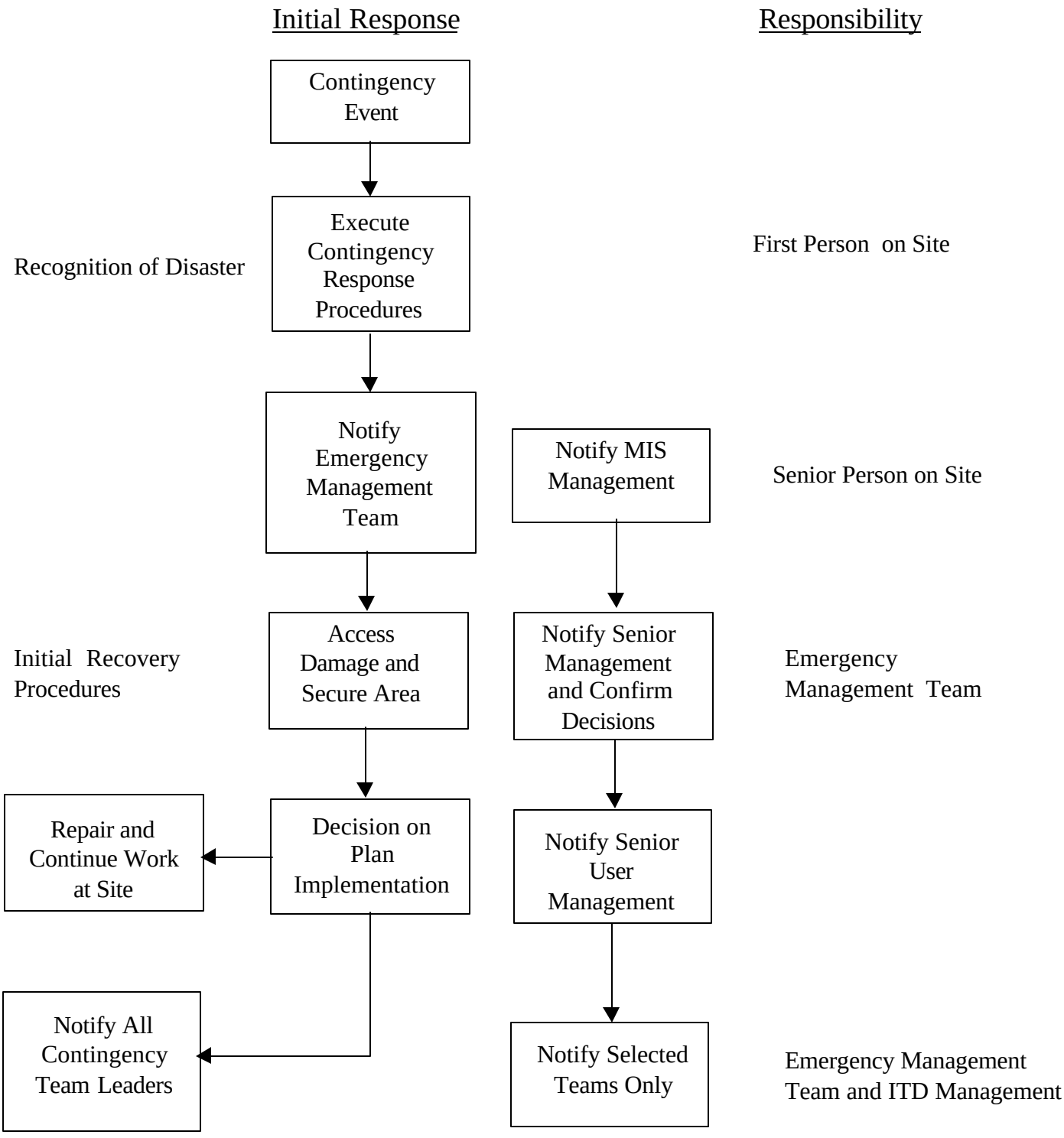
1. Loss of Power
2. Lost of Environmental controls
3. Breaches of security
4. Interruptions of internal/external communications

Steps necessary for the following disruptions in the normal flow of data and activities will not necessarily be the same since the severity of the disruption would not be the same as the above events.

5. Systems hang-up or shutdown
6. Degradation of performance
7. Irrational data presented to users
8. Produces results with incorrect, but acceptable errors
9. Files corrupted or “lost”
10. Unreliable / unpredictable results
11. Y2K repair / replacement incomplete

Items 5 through 11 require coordination between the Data Center and Programming Staff for resolution.

CONTINGENCY PLAN EXECUTION



CONTINGENCY PLAN COORDINATION

Within six hours of event

- Notify Backup site
- Notify Key personnel
- Notify intermediate user management in priority order
- Establish administrative support
- Start movement of supplies

Within 12 hours of event

- Assemble backup media and listings at backup site
- Assemble sufficient supplies and equipment at backup site

Within 24 hours of event

- Restore system pack and test system
- Start operations of critical systems
- Bring up full operating system
- Load Master files
- Test and debug system
- Have all critical processes operational
- Establish processing schedule
- Notify all concerned users
- Reassess damage

Recovery Procedures in Parallel

- Have all resources in place at backup site
- Bring up and test programs at data center
- Load data collected during contingency period
- Resume backup and off-site storage procedures
- Complete salvage efforts (if necessary)
- Debrief staff
- Report to management

- Restoration of Computerized Data

  If Payroll implements this contingency plan for the 0700 pay period or for the 2400 pay period because no wire transfer system is available, the ITD programming staff will run necessary programs to create the emergency records to post the EPA amounts given to the employees to the payroll master.

  The locations that use PTRS for time reporting will enter the time for employees, time will be certified, uploaded and a special payroll will be run to collect the EPA and pay the employees the remainder of their pay for the 0700 pay period.

  All programs will be restored, tested and returned to normal operations.

APPENDIX

RECOVERY TEAMS

- Emergency Management Team
- Data Center Operations Team
- Communications Team
- Data Entry and Control Team
- Special Projects/Administrative Services Team
- Database/Systems Software Team
- Internal Audit

Emergency (Contingency) Management Team

- Responsibilities

  - Approve the objectives, scope, and assumptions upon which the Business Continuity Plan is based.

  - Direct support of the contingency planning process by all functional areas of the organization.

  - Audit the initial contingency plan and later test the workability and the costs associated with the contingency plan.

  - Assure that the conversion to the backup operation is under sufficient audit control to provide reliability and consistency to the accounting records.

  - Assure that the necessary supervision and controls are in place during the utilization of the contingency plan.

  - Activate the Business Continuity Program (Contingency Plan) in the event of a disaster.

- Team Leader

Name: Ennis Davis
Director of Information Systems

Office Phone: _____

Home Phone: _____

Alternate Phone: _____

Pager/Cell Phone: _____

Emergency Management Team - continued

- Team Members

Name: Julio Rodriguez Director of Systems and Programming Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Richard Overturf, Deputy Director Systems and Programming Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

Emergency Management Team – continued

- Contingency Functions
  - Activate the Contingency Plan
  - Perform an internal audit in the following areas:
    - ⊗ See that the necessary controls have been imbedded in the system for preparing routine daily backup media.
    - ⊗ Determine which areas require data input, computer media, and recent output files.
    - ⊗ Run audit tests on the first backup runs shortly after they have been produced.
    - ⊗ Perform a detailed audit review of the critical accounting files after the first backup cycle has been completed.
- Preplanning Required:
  - Establishing a strong control environment in the ITD services activities.
  - Work with Systems and Programming to identify control points in the business systems and to design and document the controls.
  - Arrange for sufficient routine collection of control information so that there is a clear trail to the point of need and comparable information gathered on the backup systems.

Data Center Operations Team

- Team Members

Name: Robert F. Armendariz, Director Data Processing Operations Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Anthony Riola, Manager Data Processing, B Shift Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Javier Quinonez, Supervisor Shift A DP Operations Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Daniel Mendoza,, Supervisor Shift C DP Operations Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

Data Center Operations Team – continued

- Responsibilities
  - Assure that the data center is secure.
  - Assure that occupants have been instructed and trained in emergency procedures.
  - Assure that all employees were badges.
  - Assure that the procedure library contains all the job control necessary to execute job streams.
  - Assure that there is a formal scheduling system.
  - Assure that the following are backed-up daily and rotated offsite: Procedure Library, Tape Librarian, and Job Scheduling.

Communications Team

- Team Members

Name:	Jeanie Ray, Director Information Systems Support Branch
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name:	Irene B. Salazar, Administrator Information Systems Support
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name:	Flora L. Synigal, Manager Computer Hotline Unit
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

- Responsibilities
  - Assure that the on-line system have proper recovery procedures if the system goes down.
  - Make sure that the updating of master files are restricted to certain operations or terminals
  - Prioritized on-line input so that critical input can be entered while the contingency plan is operational.

Data Entry and Control Team

- Team Members

Name:	Gloria S. B. Brenklin Data Entry Supervisor, Shift A
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name:	Ruben Reyes, DP Operations Supervisor, Shift A
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name:	Amado Hernandez Data Control Supervisor, Shift A
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

Data Entry and Control Team – Continued

Name:	Marcos Aranda Zamora DP Operations, Shift B
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name:	Paula Yvonne West Data Control Supervisor, Shift B
	Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

Data Entry and Control Team – continued

- Responsibilities
  - Establish Data Input and Preparation services to meet the processing requirements for input.
  - Establish the Data Control functions for all necessary systems.
  - Assure that Input documents are maintained.
  - Generate necessary reports for all data processing for the aforementioned period.
  - Make sure that instructional procedures are available for data entry processes.

Database/System Software Team

- Team Members

Name: Vicki Frederick, Director System Software & Security Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Pearlie King Database Specialist Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: David Khalieque Operating System Specialist Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Scott Burnside Operating Systems Specialist Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

Database/System Software Team – continued

Name: Untung Sutrissno Operating System Specialist Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Kim Tran System Science Specialist Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____
Name: Leo Tam Systems Standards Manager Office Phone: _____ Home Phone: _____ Alternate Phone: _____ Pager/Cell Phone: _____

Database/System Software Team – continued

- Responsibilities
  - Assure that the application software is backed-up and stored offsite.
  - Make sure that there will be complete audit trails.
  - Assure that al critical files are backed-up.
  - Assure that the system has adequate controls, such as, batch totals, hash totals, run totals, and dollar amounts.
  - Assure that a list is available of al systems with the person responsible.
  - Identify the back-up person.
  - Make sure that operation run manuals are available on site.
  - Assure that standards require all programs to include proper controls and totals for complete auditing, and for detection of correction of errors.

Internal Audit Team

- Team Members

Name:	Robert Green EDP, Senior Auditor
Office Phone:	
Home Phone:	
Alternate Phone:	
Pager/Cell Phone:	

- Responsibilities

  - Assure that proper controls are established

  - Assure that all personnel have been advised about the confidentiality of all information that they work with.

Business Continuity Worksheets

DATA CENTER DISASTER RECOVERY PLAN

(THE FOLLOWING WORKSHEETS ARE COVERED BY THE DATA CENTER PLAN)

- BACKUP STRATEGY WORKSHEET FOR SMALL SYSTEMS
- TAPE BACKUP WORKSHEET
- OFF-SITE STORAGE REQUIREMENTS WORKSHEET
- TEMPORARY / ROTATING STORAGE
- USER RECOVERY CENTER REQUIREMENTS CHECKLIST
- RESOURCE REQUIREMENTS WORKSHEET
- RECORDS REQUIREMENTS
- SUPPLY AND LOGISTICS
- RECORDS RETENTION WORKSHEET
- DEPARTMENTAL NOTIFICATION DIRECTORY
- RESOURCE REQUIREMENTS WORKSHEET
- IMPACT ANALYSIS WORKSHEET
- CRITICALITY ASSESSMENT LIST
- DISASTER PREVENTION WORKSHEET
- NOTIFICATION DIRECTORY
- HARDWARE INVENTROY
- SOFTWARE INVENTORY
- RECORDS INVENTORY
- SUPPLIES/MARTERIALS INVENTORY
- USER REQUIREMENTS
- PROCEDURAL DOCUMENTATION
- RECOVERY PRIORITY AND PROCEDURE
- CHANGE MANAGEMENT FORMS

Glossary

ITEM	DESCRIPTION
Applications	A defined and named set of computer programs and data processed electronically in support of one or more business processes.
Application Controls	Methods of ensuring that only complete, accurate and valid data are entered and updated in a computer system; that processing accomplishes the correct task; that processing results meet expectations; and that data are maintained.
Application Software	Computer readable code directing the actual input, processing, and output activities for users.
Audit Trail	In computer systems, a step-by-step history of a transaction, especially a transaction with security sensitivity. Includes source documents, electronic logs, and a record of accesses to restricted files.
Auxiliary Storage	Data storage other than main memory, such as that on a disk storage unit.
Backup	A method of protecting vital records that schedules the copying or duplicating of vital records for the purpose of protection. The primary purpose of providing backup data for contingency operations is for application/systems restoration. Contingency backups are further protected by offsite storage.
Batch Processing	A method of processing data in chunks (batches). Information and instructions are put into the computer for handling as a single unit.

Business as Usual	Operating under normal conditions, i.e., without any significant interruptions of operations as a result of a disaster.
Business Continuity Plan	The advance planning and preparation that are necessary to minimize loss and ensure continuity of critical business functions of an organization in the event of business disruptions.
Business Function	The most elementary activities, e.g., calculating gross pay; updating job descriptions; matching invoices to receiving reports.
Business Impact Analysis	A study to estimate the effect that a specific disaster/incident might have on a given operation or activity.
Checklist Tests	A method used to test a completed continuity plan. This test is used to determine if information pertinent to the business process is accurate and current.
Cold Site	A backup computer site without computer hardware. All environmental components, such as power, air condition, and data communications are installed. Theoretically, a computer cold site could be operational within a few hours or days following delivery of hardware.
Critical Application	An application or system so critical to a business process that the loss of the application or system would disable a critical business function.
Critical Business Function	A business function so essential to the organization that the loss of the function would result in a loss of depletion of assets of the corporation.
Critical IT Function	An IT function critical to a business process that the loss of the function would disable a critical business function.

Critical Need	The minimal procedures and equipment required to continue operations should a department, main facility, computer center, business process, or a combination of these become inaccessible.
Critical Time Frame	**Computer Application System:** The time between the point of interruption and the point at which an application system must be updated to current status (see maximum allowable downtime).
Critical Time Frame	**Business Function:** The time between the point of interruption and the point at which the business function must have critical services operating at the minimum acceptable level.
Critical Time Periods	Description of special considerations for critical processing periods and special requirements for restoration schedules.
Declaration Fee	A one-time charge paid to a computer backup hot-site (or cold-site) provider at the time a disaster is officially declared.
Disaster	An incident of such severity and magnitude that emergency steeps are needed to stay in business.
Disaster Recovery Cycle	Consists of: (1) Normal Operations – the period of time before a disaster occurs, (2) Emergency Response – the hours immediately following a disaster, (3) Interim Processing – the period of time from the occurrence of a disaster until temporary operations are restored, and (4) Restoration – returning to normal.
Emergency Management Team	Lead or managerial personnel from key support organizations responsible for formulating organizational emergency response plans and managing emergency response activities.
Function	Business Function

Hardware Platform	A category of Information Technology resources (hardware platforms) on which critical application processing occurs.
Hot Site	A backup computer site with compatible hardware installed.
Interim Processing Guidelines	A program that outlines how specific activities will be performed until normal processing capability is restored.
Interim Processing Period	The period of time between the occurrence of a disaster and the time when normal operations are restored.
Interim Processing Strategies	A conceptual summary of Interim Processing guidelines applying to a particular business function.
Magnetic Media	A tape or disk coated with magnetic material on which data is stored.
Maximum Allowance Downtime	The longest duration of time for which a computer application could be unavailable, yet, from which an acceptable and successful recovery process could be completed. The MAD is the outage period of an application beyond which business management could not afford to see outage continue, with all financial and operational factors considered.
Mobile Site	Either a hot-site or cold-site on wheels; usually one or more large trailers.
Notification List	A list of key individuals to be contacted, usually in the event of a disaster. Notification lists normally contain phone numbers and addresses, which may be used in the event that telephones are not operational.

Offsite Location	A location usually at least several hundred yards or more from a facility that could incur a disaster.
Offsite Storage	The process of storing records at a location removed from the normal place of use; i.e., a storage location that is a sufficient distance from the location of normal use to ensure safety from the effects of a disaster. Offsite storage may be used for data, documents, lists, or any other vital records required for recovery from a disaster or for testing contingency plans. A major factor in selection of a satisfactory offsite location is the timeliness and reliability of data retrieval.
Recovery as of	The point in time (with respect to day of week, business cycles, backup schedule, etc.) to which the application need to be recovered for contingency purposes.
Reciprocal Agreement	When two different organizations mutually agree to back up each other's processing capability in the event that either on incurs a disaster.
Redundant Backup Site	Any of two or more data centers that could (by temporarily decreasing their own workload) assume the processing loan of critical applications from another data center.
Subscription Fee	Normally, monthly fees paid for the privilege of using a backup computer hot-site or cold-site, on a first-come, first-served basis.
User Preparedness Reviews	Periodic simulations of disaster recovery conditions for the purpose of evaluating how well an individual or department is prepared to cope with disaster conditions.
Vital Business Functions	Those specific business activities that have a significant impact on cash flow or servicing customer orders

Vital Record	A record that contains information essential to an organization's ability to continue or resume operations or to substantiate rights or obligations. Data files necessary to ensure that critical applications/systems can function are vital records.
Window	The length of time it is expected to take (under emergency conditions, with adequate resources) to restore whatever processing capability was destroyed in a disaster.